UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,622	03/30/2004	Kazumasa Omote	1924.70199	3471

7590 10/04/2010

Patrick G. Burns, Esq.
GREER, BURNS & CRAIN, LTD.
Suite 2500
300 South Wacker Dr.
Chicago, IL 60606

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
10/04/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/812,622	OMOTE ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,8,13,15-18,22-25,27,28,34,35,41 and 43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,8,13,15-18,22-25,27,28,34,35,41 and 43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.
Applicant's submission filed on 7-19-2010 has been entered.

2. Claims **1, 3 - 5, 8, 13, 15 - 18, 22 - 25, 27, 28, 34, 35, 41, 43** are pending. Claims **1, 3, 5, 8, 13, 15, 16, 18, 22 - 25, 27, 28, 34, 35** have been amended. Claims **2, 6, 7, 9 - 12, 14, 19 - 21, 26, 29 - 33, 36 - 40, 42** have been cancelled. Claims **1, 3, 5, 8, 13, 15, 16, 18, 22, 23, 24, 25, 27, 28, 34, 35** are independent. This application was filed on 3-20-2004.

Response to Arguments

3. Applicant's arguments have been fully considered but they were not persuasive.

3.1 The 112 Rejections for Claims **5, 18** will be maintained based on a review of the passages in the Specification, page 25, line 24 to page 28, line 7 suggested by the Applicant. These passages appear to indicate that when the number of communicated SYN packets exceeds a threshold (in the cited sections there does not appear to be a

definition as to what the threshold is set at) and the destined packets are sent to a particular IP address, then a determination that a worm is controlling communications can be made. Claims **5, 18** appear to disclose that the number of packets communicated currently is greater then the number of packets communicated at the first check for the number of packets communicated. There does not appear to be any indication of the term threshold. The indication is that the number of packets connected with a destination has increased. Spiegel discloses the determination of a worm based on network traffic considerations such as the amount of network traffic associated with a particular IP address. (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses, and information not matching criteria for normal traffic setting; col. 3, lines 20-24: connection attempts to remote destinations over a period of time; col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria) The fact that the claims were prior amended does not change the fact that for Claims **5, 18**, there is no disclosure for the limitation that all three conditions must be met before a worm can be detected.

The 112 Rejections for Claims **1, 13, 15** will be withdrawn based on amendments to remove the indicated clam limitation: *"changing the measurement parameters when the communication is judged to have been executed by the worm at the judging; wherein the acquiring includes acquiring, based on the measurement parameters changed at the changing, the information on the communication judged to have been executed by the worm at the judging".*

3.2 Applicant argues that the referenced prior art does not disclose, Independent *Claims 1, 13, 15, 3 and 16 with first and second settings and first and second predetermined criteria.*

There does not appear to be any disclosure for the terms, first setting and second setting within the specification. The specification discloses an initial setting indicated the setting before a worm has been judged (normal setting). And, the specification discloses an additional setting after a worm has been judged. (setting after detection) There does not appear there is disclosure I the specification or original claims for monitoring communications with a new setting after a worm has been determined. (See the 112 Rejections)

Spiegel discloses continuously monitoring communications traffic. Spiegel discloses that certain systems can be excluded from an alert or termination when a worm is detected. If a system falls into this category, then monitoring continues after a worm has been detected. (see Spiegel col 6, lines 7-11: excluding a particular host from alert or termination, monitoring continues after worm detection)

3.3 Applicant argues that the referenced prior art does not disclose, *Claims 5, 18 and all three conditions.*

There does not appear that there is disclosure the claim limitations that all three of the indicated conditions must be met before a worm is detected. See 112 Rejections. Spiegel discloses a set of criteria used to determine when communications is controlled

by a worm and a set of actions to perform when a worm has been detected. (See current Office Action)

3.4 Applicant argues that the referenced prior art does not disclose, *Claim 8 and type of worm executing.*

Spiegel discloses a determination of the type of worm based on history or previously recorded information. (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination; col. 6, lines 15-22: software, implementation means)

3.5 Applicant argues that the referenced prior art does not disclose, *Claims 22, 23, 24, 34, 25, 27, 28, 35 and summing number packets.*

Spiegel discloses that each packet is inspected and the extraction of feature information from the packets. It is well known in the art to generate a count of a sequence of entities. It would be well know in the art to generate a count or summation of the number of packets with a monitored traffic flow. (see Spiegel paragraph [0031], lines 1-14: inspect traffic; traffic comprises packet traffic with each packet inspected) And, Bunker discloses calculation to generate statistics for intrusion detection and the specific detection of a worm. (see Bunker paragraph [0189], lines 1-11; paragraph [0215], lines 1-5; paragraph [0220], lines 8-12: calculation (summation) of access information in worm determination)

3.6 Spiegel prior art discloses monitoring network traffic such as network packets

and analyzing the monitored traffic to determine whether the communications is from a network node infected by a worm. The analysis is completed over a period of time. (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses, and information not matching criteria for normal traffic; col. 3, lines 20-24: connection attempts to remote destinations over a period of time)

Siegel prior art discloses a determination that communication is executed by a system infected by a worm. Spiegel prior art and its combination with Willebeek-LeMair and Bunker disclose the criteria of a large number of packets and additional criteria used to make the determination of communication from a system infected by a worm. (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses and information not matching criteria for normal traffic setting; col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

Spiegel prior art discloses that previously recorded information or historical information can be analyzed and compared to current communication information in order to make a determination of whether communication is coming from an infected worm. (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination) In addition, threshold limitations in data processing disclose a comparison of a current parameter value against a threshold value to determine a course of action.

Spiegel prior art discloses the usage of threshold criteria to make a determination

of communication from a system infected by a worm. A threshold is maximum limit parameter. A current count of communication packets for connection attempts must be counted or summed and the current count of these types of packets are compared against a limit or threshold parameter.

Willebeek-LeMair prior art discloses the specific extraction of reference information such as a port number from a communications packet. Willebeek-LeMair prior art discloses the usage of port number information in the analysis of communication traffic. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number))

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims **1, 3, 13, 15, 16** and **5, 18** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

For Claims **5, 18** there is no disclosure for the amended limitation: “all three conditions are satisfied”. There is no disclosure for this claim limitation in the specification or the original claims.

For Claims **1, 3, 13, 15, 16**, there does not appear to be disclosure for the following claims limitation "wherein the acquiring includes acquiring information of the monitored communication, based on second setting information for the plurality of setting items after the monitored communication judged to have been executed by the worm at the judging". The specification does not appear to address monitoring the previously monitored communication link with the new threshold parameter that was used to identify the worm and collecting information over communication link after worm detection.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims **15 - 18, 24, 28, 34, 35** and **1, 3 - 5, 8, 22, 25, 41, 43** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter as follows.

Claims **15 - 18, 24, 28, 34, 35** are to be construed as a computer system of *"software per se"*, unless the specification makes clear the only reasonable interpretation of the word *"computer system"* includes at least one tangible hardware inclusive component. Applicant must indicate at least one tangible hardware components such as a memory for storage of program instructions.

Claims **1, 3 - 5, 8, 22, 25, 41, 43** are rejected under 35 USC 101 since the

claims are directed to non-statutory subject matter. Claims **1, 3 - 5, 8, 22, 25, 41, 43** recite computer readable recording medium which appear to cover both transitory and non-transitory embodiments. The broadest reasonable interpretation of a claim drawn to a computer readable recording medium (also called machine readable medium and other such variations) typically covers forms of non-transitory tangible media and transitory propagating *signals per se* in view of the ordinary and customary meaning of computer readable media. The Examiner suggests that the Applicant add the limitation "non-transitory" to the computer readable recording medium as recited in the claim(s) in order to properly render the claim(s) in statutory form in view of their broadest reasonable interpretation in light of the originally filed specification. The Examiner also suggests that the specification may be amended to add the term "non-transitory computer readable recording medium" to avoid a potential objection to the specification for a lack of antecedent basis of the claimed terminology.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims **1, 3 - 5, 8, 13, 15 - 18, 22 - 24, 34, 41, 43** are rejected under 35

U.S.C. 103(a) as being unpatentable over **Spiegel et al.** (US Patent No. **7,159,149**) in view of **Willebeek-LeMair et al.** (US PGPUB No. **20030204632**).

With Regards to Claims 1, 13, 15, Spiegel discloses a computer readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

a) acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet based on first setting information for a plurality of setting items. (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses, and information not matching criteria for normal traffic setting; col. 3, lines 20-24: connection attempts to remote destinations over a period of time; col. 2, lines 51-53; col. 2, lines 62-65; col. 6, lines 15-22: software, implementation means)

Furthermore, Spiegel discloses:

b) judging whether the monitored communication has been executed by the worm based on the information acquired and a predetermined judgment criteria; (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

e) wherein the acquiring includes acquiring information of the monitored

communication, based on second setting information for the plurality of setting items after the monitored communication judged to have been executed by the worm at the judging. (see Spiegel col. 5, lines 15-21: dynamic (i.e. adjustable, changeable) parameters used for worm determination; col. 5, lines 47-53: heuristic can be fine tuned; col. 6, lines 15-26: software, implementation means; col. 5, lines 38-42: threshold (parameters) can be easily reconfigured; parameters can be set based on system requirements; col 6, lines 7-11: excluding a particular host from alert or termination, monitoring continues after worm detection)

Spiegel does not specifically disclose extracting specific information and blocking communication packet.

However, Willebeek-LeMair discloses:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm at the judging; (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number))

d) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting. (see Willebeek-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments

(inside network segment and outside network segment))

It would have been obvious to one of ordinary skill in the art to modify Spiegel for extracting specific information and blocking communication packet as taught by Willebeek-LeMair. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair for threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

With Regards to Claims 3, 16, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

a) acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for first setting information for a plurality of setting items; as stated in Claim 1 above.

Furthermore, Spiegel discloses for following:

b) judging whether the communication has been executed by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above;

e) wherein the judging includes further judging whether the monitored communication has been executed by the worm after the monitored

communication is judged to have been executed by the worm at the judging, based on the information acquired and a second predetermined judgment criteria. (see Spiegel col. 5, lines 8-10; col. 5, lines 15-21: worm determination based on information and adjusted (i.e. changed) information; col. 6, lines 15-22: software, implementation means; col 6, lines 7-11: excluding a particular host from alert or termination, monitoring continues after worm detection)

Spiegel does not specifically disclose extracting information and blocking communication.

However, Willebeek-LeMair discloses the following:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm at the judging; as stated in Claim 1 above;

d) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting as stated in Claim 1 above.

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claims 4, 17, Spiegel discloses the computer readable recording medium, device according to claims 1, 15, the judging includes judging that a

communication from a computer that is in the predetermined network segment is executed by the worm when there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 3, lines 20-27: network communication packets throughput increased, worm determination; col. 4, lines 17-22: number of destination addresses is high; col. 6, lines 15-22: software, implementation means)

With Regards to Claims 5, 18, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

a) acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet based on first setting information for a plurality of setting items; as stated in Claim 1 above.

Furthermore, Spiegel discloses the following:

b) first judging whether a computer in the predetermined network segment is infected by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above;

c) second judging whether a plurality of computers in the predetermined network

segment are infected by the worm; (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses, and information not matching criteria for normal traffic setting; col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored)

f) the second judging includes judging that plurality of computers in the predetermined network segment are infected by the worm all three conditions are satisfied, the three conditions being that; (see Spiegel col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored)

g) a monitored communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging; (see Spiegel col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored; col. 6, lines 15-22: software, implementation means)

h) a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging, and a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging. (see Spiegel

col. 3, lines 20-27: worm determination based on number of packets transferred to addresses (i.e. inside or outside local network); connection attempts (destination addresses))

Spiegel does not specifically disclose extracting information and blocking communication.

However, Willebeek-LeMair discloses the following:

d) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the first judging that the computer is infected by the worm; as stated in Claim 1 above;

e) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting; as stated in Claim 1 above.

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claim 8, Spiegel discloses a computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

a) acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet based on first setting information for a plurality of setting items; as stated in Claim 1 above.

Furthermore, Spiegel discloses the following:

b) judging whether the monitored communication is executed by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above;

e) wherein the judging includes identifying a type of the worm executing the monitored communication by comparing features of monitored communication with features of communication executed by a worm that are recorded in advance. (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination; col. 6, lines 15-22: software, implementation means)

Spiegel does not specifically disclose extracting information and blocking communication.

However, Willebeek-LeMair discloses the following:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged at the judging that the monitored communication is executed by the worm; as stated in Claim 1 above;

d) blocking the communication packet that is transmitted between the

predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting; as stated in Claim 1 above.

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claims 22, 23, 24, 34, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

a) acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet based on first setting information for a plurality of setting items; as stated in Claim 1 above.

Furthermore, Spiegel discloses:

b) judging whether the monitored communication has been executed by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above.

Spiegel does not specifically disclose extracting port information and blocking communication.

However, Willebeek-LeMair discloses the following:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm at the judging; as stated in Claim 1 above;

d) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting; as stated in Claim 1 above;

e) wherein the extracting includes summing up a number of communication packets for each port number, the communication packets being transmitted in the monitored communication being executed by the worm, and extracting as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication judged to have been executed by the worm. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number))

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claim 41, Spiegel discloses the computer-readable recording medium according to claim 3, the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm based on communication packets as well as number of destination addresses of

communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 1, lines 50-62: connections attempts (communication packets) directed to a destination address used in determination of a worm)

Spiegel does not specifically disclose an increase in number of communication packets that are transmitted.

However, Willebeek-LeMair discloses an increase in number of communication packets that are transmitted. (see Willebeek-LeMair paragraph [0007], lines 8-12: large numbers of packets and connection requests (destination address))

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claim 43, Spiegel discloses the computer-readable recording medium according to claim 8, the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm based on communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 1, lines 50-62: connections attempts (communication packets) directed to a destination address used in determination of a worm)

Spiegel does not specifically disclose an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted.

However, Willebeek-LeMair discloses an increase in number of communication packets

as well as number of destination addresses of communication packets that are transmitted. (see Willebeek-LeMair paragraph [0007], lines 8-12: large numbers of packets and connection requests (destination address))

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

10. Claims **25, 27, 28, 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Spiegel-"Willebeek-LeMair"** and further in view of **Bunker et al.** (US PGPUB No. **20030056116**).

With Regards to Claims 25, 27, 28, 35, Spiegel discloses the computer program, computer-readable medium, method, and device according to claims 1, 12, 13, 14, 33. (see Spiegel col. 1, lines 48-62: monitoring for worm determination; col. 4, lines 45-48: traffic analysis, calculation utilizing network addressing (IP address, port number)) a computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

a) acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet based on setting information including unit time for first setting information for a plurality of setting items; as stated in Claim 1 above.

Furthermore, Spiegel discloses:

b) judging whether the monitored communication is executed by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above.

Spiegel does not specifically disclose extracting information such as a port number and blocking communication.

However, Willebeek-LeMair discloses the following:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged at the judging that the monitored communication is executed by the worm; as stated in Claim 1 above;

d) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting; as stated in Claim 1 above.

Spiegel does not specifically disclose calculations utilizing reference information such as port numbers in the analysis of work determination.

However, Bunker discloses

e) wherein extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the monitored communication being executed by the worm, and extracting, as the reference information, a direction of the monitored communication, the number of

the communication packets is over a threshold value. (see Bunker paragraph [0189], lines 1-11; paragraph [0215], lines 1-5; paragraph [0220], lines 8-12: calculation (summation) of access information in worm determination)

It would have been obvious to one of ordinary skill in the art to modify Spiegel to calculate a summation of reference information utilized for worm determination as taught by Bunker. One of ordinary skill in the art would have been motivated to employ the teachings of Bunker to emulate hacker methodology in a safe way and enable study of network security openings without affecting customer operations. (see Bunker paragraph [0012], lines 1-8)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
September 13, 2010